AGENCY OF HUMAN SERVICES

AHS Risk Assessment Standard

Jack Green

10/17/2013

The purpose of this procedure is to facilitate the implementation of the Vermont Health Connect's security control requirements for the Risk Assessment (RA-1, RA-2, RA-3) Controls.

Revision History

Date	Version	Description	Author
	.99	Draft received from HI and reviewed by Referentia	
	1.0	Created Document	AHS
8/16/2013	2.0	Document revised for VHC standards	Jack Green
10/17/2013	3.0	Procedures reviewed and adapted for VHC business processes and security requirements	Jack Green

PURPOSE/STANDARD STATEMENT:

The purpose of this procedure is to facilitate the implementation of the Vermont Health Connect's (VHC) security control requirements for the Risk Assessment (RA-1, RA-2, RA-3) Controls.

The information systems covered in this procedure document contain but are not limited to the following:

- VHC website
- VHC Portal
- VHC workstations and mobile phones
- Network Accounts
- E-Mail accounts

SCOPE

The scope of this standard includes the VHC and its constituent systems only

STANDARD

Risk Assessment

1. Assessments must be conducted to evaluate the level of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.
    i. The authorization boundary is a prerequisite and must be clearly defined before beginning the risk assessment.
2. The Risk Assessment must take into account vulnerabilities, threat sources, and security controls planned or in place to determine the resulting level of residual risk to organizational operations, organizational assets, individuals, and other organizations.
    i. The Risk Assessment must take into account risks posed to VHC operations, VHC's assets, or individuals from external parties, including but not limited to:
        1. Entities such as foreign nations and business competitors that may have an interest in information supplied to VHC.
        2. Service providers.
        3. Contractors operating information systems on behalf of the Agency.
        4. Individuals accessing VHC's information systems.
        5. Outsourcing entities.

   ii. The Risk Assessment must address public access to federal information systems and include risks associated with electronic authentication, if this is applicable.
   iii. The Risk Assessment must factor in incident information, results and trends of continuous monitoring, penetration testing, and vulnerability scanning efforts.
   iv. The Risk Assessment must factor in the status of POA&Ms for the information system.
   v. The Results after completing a Risk Assessment should be documented in the Risk Assessment Report (RAR).

3. Risk assessments must be a collaborative effort among representatives of management, operational, technology and information security disciplines.
4. The risk assessment results must be documented in the Risk Assessment Plan or the System Security Plan.
5. The VHC Security Manager must ensure that a risk assessment is conducted for the following reasons:
   i. Whenever high impact weaknesses are identified;
   ii. Every three (3) years;
   iii. Whenever modifications are made to sensitive information systems, or to their physical environments, interfaces, or user community.
6. The risk assessment shall consider the effects of the modifications on the operational risk profile of the information system.
7. SSPs shall be updated and re-certification conducted if warranted by the results of the risk assessment.
8. The following are the specific criteria (but not limited to these criteria) for what is considered a significant change to the information system:
   i. A change to the operating environment of a major information system that alters the overall level of risk previously authorized by the AO.
   ii. A change to the threat environment.
   iii. A change in the IT system's physical environment.
   iv. A significant change to the software or hardware.
   v. A breach of the information system's security that could possibly invalidate the authorization.
   vi. A change with respect to interconnected systems.
   vii. A change in the security categorization level.
9. The Risk Assessment must be reviewed and, if necessary, updated:
   i. As part of the change management activities for the information system.
   ii. At least annually.
10. The document review history of the Risk Assessment must be updated to reflect the date the review was performed.
11. The results of the annual review must be reported to the AO.

12. Risk Executives shall review recommendations for risk determinations and risk acceptability and may recommend changes to the AO and appropriate CIO.
13. If at any time during the risk assessment a potential threat or vulnerability that presents a critical risk to the system or its assets, must be brought to the immediate attention of the SO for corrective or mitigating action.
14. A POA&M must be created for the corrective action.
    i. The changes documented in the POA&M must be implemented.
    ii. A follow-up analysis must be conducted to determine whether the changes made adequately mitigate the vulnerabilities.
15. The following sections must be included in the Risk Assessment:
    i. System Characterization.
    ii. Control Review – Vulnerabilities.
        1. Each control required by NIST SP 800-53, Revision 3 must be listed, including the implementation status (i.e., not in place, planned, in place) of the control.
        2. Controls that are in place may be tentatively considered to be of low risk pending further analysis.
        3. Controls that are either planned or not in place must be considered to have at least moderate or high risk since they constitute vulnerabilities.
    iii. Threats
        1. Threat(s) must be identified for each vulnerability.
        2. The threat sources for each threat must be identified and analyzed in terms of threat actions and potential consequences.
    iv. Likelihood
        1. The likelihood that a threat will be exercised against the vulnerability must be identified for each vulnerability.
        2. The likelihood must at least be expressed in qualitative terms such as high, medium, or low.
    v. Impact Analysis
        1. The impact analysis assesses the potential adverse consequences of a threat being exercised for an identified vulnerability.
        2. The impact analysis must consider:
            a. The mission or business impact analysis (BIA) of the functions of the organization supported by the system and its information.
            b. The criticality (i.e., importance to the organization) and sensitivity of both the information system and its information.
    vi. Risk Analysis
        1. For each vulnerability/threat pair, the risk level (i.e., high, medium, or low) must be calculated using the method described in NIST SP 800-30 and documented for the Risk Assessment report.

2. The calculated risk levels must be used to prioritize risks and determine which ones justify a recommendation for further mitigating controls.

vii. Control Recommendations
   1. Controls that can mitigate the identified risks in accordance with the needs of the organization’s operations must be identified.

viii. Summary
   1. The results of the assessment must be summarized and documented as part of the Risk Assessment report. This includes the number of high, medium, and low risks, as well as the overall level of system risk.
   2. The final Risk Assessment report must provide a conclusion that includes an overall risk statement.

16. The risk assessment results must be considered privileged information, to be shared only with authorized individuals.
17. Copies of the Risk Assessment report must be provided to the SAISO and Information Security Officer (ISO) for review and comment. The SAISO or ISO may require additional controls, enhancements, or mitigations as needed.
18. The Risk Assessment report must be presented to the System Owner (SO), the AO, other appropriate IT and physical security directors, and Information System Security Officer (ISSO) for their review and appropriate action.
19. The outstanding risks must also be presented to designated information security personnel and management of related GSSs, MAs, and interconnected systems, if any, since the risks may affect the risk profile of their information system.
20. The AO must be informed if the acceptable level of risk already established for the information system changes.
21. The results of the Risk Assessment must be used as follows:
    i. The risk must be considered when scoping the applicability of individual security controls in the control baseline (derived from the security categorization).
    ii. If a risk-based decision is made, the reasons for doing so must be documented and communicated to appropriate management officials within the organization.
    iii. If the system is under development and not yet implemented, the implementation descriptions for controls in the SSP must address how the risk(s) will be mitigated.

Security Categorization

1. The information and information system must be categorized in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

    a. The authorization boundary is a prerequisite and must be clearly defined before beginning the security categorization.
    b. The security categories are based on the potential impact should certain events occur that jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. The following potential adverse impacts must be considered:
        i. Impacts to other organizations.
        ii. National-level adverse impacts, in accordance with the USA PATRIOT Act and Homeland Security Presidential Directives.

2. The full security categorization results, and supporting rationale, must be documented and included in the System Security Plan (SSP) for the information system.
    a. If Privacy Act information is processed, stored, or transmitted by the information system, the system categorization documentation for that information and information system must accurately reflect this fact.
        i. A System of Records Notice (SORN) and designated number must also be identified in the SSP.
    b. Categorization information must be consistent and coordinated with information found in VHC's official inventory system (i.e., READ) and Capital Planning, Investment Control (CPIC) documentation and the Agency's FISMA reporting and tracking system.
3. The security categorization process must be conducted as an organization-wide activity.
    a. The programmatic Information Owner (IO), related staff, management, mission owner, System Owner (SO), and information security staff knowledgeable in the information created or collected by the program shall assist with the development of the security categorization and the organization's mission requirements and responsibilities.
    b. The Chief Information Officer (CIO) or designee and Chief Information Security Officer (CISO) or designee must be involved to provide a perspective of organization-wide risk management.
    c. Other SOs need to be apprised of and even involved with the security categorization of an information system, if they are responsible for any of the following:
        i. A General Support System (GSS) that the information system relies upon.
        ii. A Major Application (MA) that inherits controls from the information system.
        iii. An interconnected system or system that shares information with the information system.

4. Security categorization must be part of the system development life cycle (SDLC) and must meet the following requirements:
    a. Developed early in the initiation stage to ensure that the appropriate controls can be planned and implemented throughout the SDLC.
        i. The results of information and information system categorization must be used to identify the initial or baseline security controls.
    b. Reviewed and updated throughout the life cycle stages prior to security authorization and when changes occur in the information being processed in the information system.
    c. Correct for the assessment process to ensure a valid authorization.
    d. Reviewed at least annually after security authorization, and updated if necessary.
        i. The document review history of the annual system categorization must be updated to reflect the date the review was performed.
    e. Reviewed and updated if necessary whenever there is a change in the information processed in the information system, including adding, altering, or removing information.
        i. Any categorization changes may require modifications of controls, revision of risk assessments and additions to the Plan of Action and Milestones (POA&Ms), including possibly security re-authorization.
5. Information system categorizations must be reviewed and approved by management officials using the following guidelines:
    a. Throughout the development life cycle to ensure the categorization is current and reflective of the information being considered for processing in the information system.
    b. At least annually or upon implementation of the information system.
    c. Whenever there is a change in the information processed in the information system, including adding, altering, and removal of information.
6. Proper security categorization must rely upon accurate and complete analysis of the programmatic/mission information stored, processed, or transmitted by the information system.
7. For each information type, the potential impact on confidentiality, integrity and availability of the information should be included.
8. The VHC defines nine (9) major classes of information where confidentiality may be impacted:
    a. Confidential Business Information (CBI).
    b. Confidential Agency Information (CAI).
    c. Privacy Act information.
    d. Personally Identifiable Information (PII).
    e. Federal Tax Information (FTI)
    f. Enforcement-confidential information.

   g. Budgetary information prior to OMB release.
   h. Other information that is exempt from disclosure under the Freedom of Information Act (FOIA).
   i. Controlled Unclassified Information (CUI).
9. Any information system processing PII associated with a Privacy Act System of Records or containing sensitive PII must have a system categorization of moderate or high in accordance with special factors affecting the confidentiality impact level.
10. The highest categorization—also known as the high water mark—determines the overall security categorization for the information system.
    a. Applications with a security categorization of moderate or high are considered de facto major applications.
    b. Applications with a security categorization of low are generally not considered major applications, but must be specifically identified in the associated GSS SSPs.
11. When an information system—typically, a GSS—provides security or processing capabilities for one or more other information systems, then the highest security categorization level of any supported system must also be applied to the system that provides security or processing capabilities.
12. For nationally deployed information systems, the FIPS 199 security categorization must be established by the VHC program or regional organization responsible for the information system and must be monitored and updated, as needed, during the system's life cycle.
13. For systems containing PII, the confidentiality security objective shall be assigned an impact level of moderate or higher.
14. The security categorization decision must be reviewed and approved by the Authorizing Official (AO) or AO designated representative.

IMPORTANT INFORMATION

These procedures can be found at http://dvha-intra.ahs.state.vt.us/policies-protocols/InfoSec